

REMARKS

In accordance with the foregoing, claims 11 and 23 are amended. Claims 11, 14-15, 17, 20-21, and 23 are pending and under consideration.

Favorable reconsideration of this application, in light of the following discussion and in view of the present amendment, is respectfully requested.

This amendment is believed to place the application in condition for allowance, and entry therefore is respectfully requested. In the alternative, entry of this amendment is requested as placing the application in better condition for appeal by, at least, reducing the number of issues outstanding.

Entry of Amendment under 37 C.F.R. § 1.116

The Applicant requests entry of this Rule 116 Response because the amendment does not significantly alter the scope of the claims and places the application at least into a better form for purposes of appeal. No new features or new issues are being raised.

The Manual of Patent Examining Procedures (M.P.E.P.) sets forth in Section 714.12 that "any amendment that would place the case either in condition for allowance or in better form for appeal may be entered." Moreover, Section 714.13 sets forth that "the Proposed Amendment should be given sufficient consideration to determine whether the claims are in condition for allowance and/or whether the issues on appeal are simplified." The M.P.E.P. further articulates that the reason for any non-entry should be explained expressly in the Advisory Action.

CLAIM REJECTIONS UNDER 35 U.S.C. §103

Claims 11, 14-15, 17, 20-21, and 23 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No. 2003/0009659 to DiSanto et al. (hereinafter "DiSanto") in view of the article "*Conversational IP multimedia Security*" by Blom et al. ("Blom").

Independent claim 11 recites:

A security module for encrypting a telephone conversation between at least one first telecommunication terminal using a Voice over IP (VoIP) system in a packet-oriented data network, and at least one second telecommunication terminal in a public switched telephone network that is distinct from the packet-oriented data network and that is at least one of analog and digital and is connected to the packet-oriented network via a gateway, said security module being connected into a connecting line of one

of the first and second telecommunication terminals and comprising

a protocol processing unit processing data packets transported on the packet-oriented network using the encrypted transport protocol with keys for the encrypted transport protocol exchanged using a key exchange protocol, converting voice signals, created by the one of the first and second telecommunication terminals at which said security module is connected, into data packets for transport via the encrypted transport protocol and converting data packets, arriving at said security module after transport via the encrypted transport protocol, into voice signals;

a modem connection unit, used when said security module is connected in a connecting line at a second telecommunication terminal, setting up a modem connection between the second telecommunication terminal and at least one of a gateway and another second telecommunication terminal, with the data packets being transported using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection, wherein

a point-to-point protocol connection is used over the modem connection in transporting the data packets using the encrypted transport protocol, as well as messages of the key exchange protocol, and

the encrypted transport protocol is Secure Real Time Transport Protocol.

As such, claim 11 provides a protocol processing unit that processes data packets transported on the packet-oriented network using the encrypted transport protocol with keys for the encrypted transport protocol exchanged using a key exchange protocol. Furthermore, claim 11 includes a modem connection unit, used when the security module is connected in a connecting line at a second telecommunication terminal, that transports the data packets using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection. As such, the security module of claim 11 provides for end-to-end encryption between a client in a packet-oriented network and a client in a public switched telephone network (analog or digital), which is distinct from the packet-oriented network, using the key exchange protocol and the encrypted transport protocol (SRTP) because each of the two distinct networks distinctly use the key exchange protocol and the encrypted transport protocol via the claimed protocol processing unit and modem connection unit, respectively. These features are not taught by either DiSanto or Blom.

Furthermore, the modem of DiSanto does not correspond to the claimed modem connection unit, as indicated by the Examiner. As discussed above, the claimed modem connection unit when the security module is connected in a connecting line at a second PSTN

telecommunication terminal for transporting the data packets using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection. As such, the claimed modem connection unit provides a transfer of encrypted communications from the packet-oriented network into the PSTN because the packet-oriented network also uses the encrypted transport protocol with keys for the encrypted transport protocol exchanged using the key exchange protocol.

DiSanto merely discloses a security device for secure communication over a plurality of networks (see DiSanto's Abstract). The internal modem 240 in FIG. 2B of DiSanto is used to perform analog to digital conversion when digitized voice data is directed to port 245 (see paragraph [0033] of DiSanto). Thus, the modem 240 is used merely to comply with the technical requirements of a respective network, but does not provide a technical solution enabling encryption of voice data in a heterogeneous network including a packet-oriented network and a PSTN.

Furthermore, claim 11 specifies that "a point-to-point protocol connection is used over the modem connection in transporting the data packets using the encrypted transport protocol, as well as messages of the key exchange protocol." The Examiner alleges that this feature is anticipated by "a procedure for establishing a direct connection between two nodes" disclosed in DiSanto. However, unlike in DiSanto, the modem of the claimed security module enables the data packets from the packet-oriented network to be transported using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection. The procedure for establishing a direct connection between two nodes in DiSanto does not anticipate or render obvious this type of connection among terminals of different networks.

At least for the above reasons, amended claim 11 and pending claims 14-15, 17, and 20-21 depending from claim 11 patentably distinguish over the prior art.

Claim 23 recites:

A method performed by a security module for encrypting a telephone conversation between at least one first telecommunication terminal using a Voice over IP (VoIP) system in a packet-oriented data network and at least one second telecommunication terminal in a public switched telephone network that is distinct from the packet-oriented data network and that is at least one of analog and digital and is connected to the packet-oriented network via a gateway, said security module being connected into a connecting line of one of the first and second telecommunication terminals and comprising processing data packets transported on the packet-oriented

network using the encrypted transport protocol with keys for the encrypted transport protocol exchanged using a key exchange protocol, converting voice signals, created by the one of the first and second telecommunication terminals at which said security module is connected, into data packets for transport via the encrypted transport protocol and converting data packets, arriving at said security module after transport via the encrypted transport protocol, into voice signals;

when said security module is connected in a connecting line at a second telecommunication terminal, setting up a modem connection between the second telecommunication terminal and at least one of the gateway and another second telecommunication terminal, with the data packets being transported using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection; and

using a point-to-point protocol connection over the modem connection in transporting the data packets using the encrypted transport protocol, as well as messages of the key exchange protocol, wherein

the encrypted transport protocol is Secure Real Time Transport Protocol.

It is respectfully submitted that the cited prior art does not teach each of the features of claim 23, so that claim 23 patentably distinguishes over the prior art.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

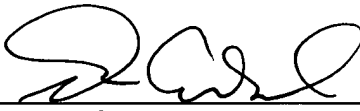
Serial No. 10/580,954

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 9-8-0

By: 
Aaron C. Walker
Registration No. 59,921

1201 New York Avenue, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501